UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,440	05/23/2001	Masahiro Takagi	208915US2RD	8894

22850 7590 02/17/2006

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 02/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/862,440	TAKAGI ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' amendment received on November 28, 2005.

2. Claims 1, 19 and 21 are amended.

3. Applicants' arguments have been fully considered but they are not persuasive.

4. Applicants on page 14, lines 4-9 of the remarks argue: "Inoue fails to disclose or suggest the feature that a gateway re-encrypts the decrypted packets obtained from decrypting the received packets before sending them to a destination device. That is, Inoue fails to disclose or suggest a gateway that receives encrypted packets and then decrypts the encrypted packets and then re-encrypts the decrypted packets and then sends this encrypted packets."

In response to above argument, Inoue discloses (see col. 2, lines 45-49 and Fig. 1) that an encrypted packet passes through Internet 6 and arrives at the gateway 4a of Home Network 1a. The packet is decrypted at the gateway 4a and is sent to the Home Agent 5 and then returns to the gateway 4a. The gateway 4a encrypts the packet again (or re-encrypt) and afterward the gateway 4a transmits the re-encrypted packet to the mobile computer 2 that is located at the visited Network 1b. Fig.1 depicts the path of the encrypted packet with dotted arrows and the path of the decrypted packet with solid arrows. Inoue further discloses (see col. 5, lines 25-30) that the same conventional

operation that is applied in Fig.1 and Fig. 2 is also implemented in his present invention. Thus, Inoue invention and its prior art employ a gateway that decrypts an encrypted packet and then re-encrypts the decrypted packet before sending to the mobile computer at a new location.

5. Applicants on page 15, lines 4-9 of the remarks argue: "Inoue fails to disclose or suggest data decryption unit configured to obtain decrypted data by decrypting the encrypted data by using the information regarding the security association and to check a destination address included in a header of the decrypted data at a time of relaying the communications with data secrecy between the first terminal device and the second terminal device' as recited in Applicants' amended Claims 1,
19 and 21."

In response to above argument, as described above Inoue employs a gateway that decrypts the encrypted packets and later re-encrypts the packets before transmitting the packets to the mobile computer. It is inherent in Inoue's invention that the gateway must utilize a cryptographic algorithm with associated keys and parameters for performing this decryption/encryption process. It is also inherent that Inoue's gateway must check the header of the packets in order to determine the destination of the packets. However, Caronni expressly discloses (see col. 6, lines 10-25) that the packet headers are checked by the gateway in order to obtain the destination address. Caronni also discloses (see col. 6, lines 10-25) that the gateway performs encryption/decryption function on secure data packet after analyzing them. This implies

that based on a security association (see also col. 5, lines 62-66) the encryption/decryption function is performed.

It is obvious that a person of ordinary skill would be motivated to combine the teachings of Inoue and Caronni to accomplish what the claimed invention is delivering.

6. Applicants on page 15, line 24 through page 16 line 2 of the remarks argue: "Caronni fails to disclose or suggest any data relaying operation, let alone Applicants' recited relay at a transport or upper layer according to the decrypted data."

In response to above argument, Caronni discloses as shown in Fig. 3 and Fig. 5 (see also col. 6, lines 18-25) that the gateway has a unit 303 that decrypts the data packets that being received then analyzed by the device 301 of the gateway; the destination address is determined and afterward the data packet is sent to its destination. Of course, in Fig. 3 the arrows indicate the direction of the outbound packets. For the outbound packets, the packets are analyzed first by device 301 and then encrypted by device 303 before transmitted to a destination. Caronni further discloses that the packets are forwarded through the protocol layers of ISO/OSI network, which corresponds to the recited relaying operation at a transport or upper layer. Inoue also teaches that the packets are relayed between two communicating devices by applying encryption and authentication processing, which functionally equivalent to the recited relaying operation at a transport or upper layer (col. 3, lines 60-67).

7. Applicants on page 16, lines 4-7 of the remarks argue: "Caronni does not encrypt the data according to the information regarding the security association."

In response to above argument, Caronni discloses as shown in Fig. 3 that the outgoing data packets are analyzed first by the device 301 and then encrypted at the device 303. The packets are analyzed to determine that whether the packet intended for a secure destination to be encrypted (see col. 6, lines 15-25). The key information used for encryption is included in a field in the header of the packets. Obviously the key information is the security association between the mobile machine and the secure network (col. 5, lines 62-67) because the key itself cannot be the key information in the header of the packets otherwise it would be read by an eavesdropping person. Thus, Caronni encrypts the data packets according to the information (i.e., an encryption key) regarding the security association read from the packet header.

8. Applicants on page 16, lines 7-10 of the remarks argue: "Applicants' Claims I 0, 20 and 22 recite an authentication function to attach authentication information to data to be transmitted to the second terminal device or the first terminal device according to the information regarding the security association. Caronni fails to disclose or suggest such an authentication operation."

In response to above argument, the same response as stated under 7 above is applied here. Moreover, Caronni discloses that the packets are being authenticated at the receiving terminal by using the key information read from a field in the packet header (see, for example, col. 6, lines 20-25).

9. In light of the above submission the previous rejection of the original claims while taking into account the claims amendments are presented as follows.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caronni (6,507,908 B1) in view of Inoue et al (6,170,057 B1; hereinafter Inoue).

Caronni discloses a secure system for transferring packets between a mobile terminal and a host terminal located in a network via a gateway (see abstract; col. 4, lines 26-37; Fig. 2).

Inoue discloses a method for encryption and authentication of packets transmitted to and from a mobile terminal to another computer in a computer network (see abstract and Fig. 1).

Regarding claims 1, 10 and 19-22, Caronni discloses a gateway that forwards the data packets on to higher network layers includes a packet analysis device (corresponding to the recited a security information management unit), which monitors

the addresses of inbound and outbound packets to a mobile machine outside of a secure network having a security association (col. 5, lines 57-67; col. 6, lines 27-55). Caronni further discloses (see col. 6, lines 10-25) that the packet headers are checked by the gateway in order to obtain the destination address. The analysis device extracts key information from packet headers to determines the corresponding secure IP addresses related to the cryptography of the packets (corresponding to the recited to manage information regarding a security association set up between to communicating terminals) (see col. 3, lines 40-62; col. 6, lines 30-36; col. 6, lines 52-60; col. 7, lines 59-67). Caronni also discloses that the gateway includes a unit for encrypting outgoing packets received from a device coupled to a secure network and decrypting incoming packets received from a device coupled to an insecure network using associated encryption keys that maybe maintained in a database and transmitting the packets to the destination terminal (see col. 8, lines 20-35 and Fig. 3, device 303). Caronni further discloses that the gateway has a function of forwarding the data packets to the higher network protocol layer based on the packet IP header examination and after decrypting the packet (corresponding to the recited data relay unit perform the data relaying at the transport or upper layer based on the decrypted data) (see col. 1, lines 30-40; col. 3, lines 50-62; col. 4, lines 17-25; col. 7, lines 46-58). The data packets are transmitted containing information needed for authentication (see col. 6, lines 21-26; col. 7, lines 28-37).

Caronni, however, does not expressly disclose that re-encrypting the decrypted packets obtained from decrypting the received packets before sending them to a destination device.

Inoue discloses a gateway with a data packet relaying function based on the encryption information (corresponding to the recited according to the received data) that decrypts the received encrypted data packets from a device coupled to a network and re-encrypts the same data packets before transmitting to another device coupled to a different network (see col. 2, lines 42-49; col. 5, lines 30-42). Inoue further discloses that the home agent of the home network of the mobile computer encapsulates the packet destined to the original address with a packet destined to the current location address of the mobile computer (col. 2, lines 27-37). Obviously it is inherent in Caronni that if the mobile machine does not move to a new location at a visited network, there would be no need for encapsulation pf the packets i.e., no new address would be attached to the packet to be transmitted. Inoue also discloses that the gateway has an authentication unit that authenticates the received data packets based on authentication code attached to the packet (see col. 5, lines 43-50; col. 7, lines 55-65).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the re-encryption operation of the decrypted data packets in the gateway as taught in Inoue in the system of Caronni because it would protect the data packets while being transmitted to a device coupled to an insecure network (Inoue, col. 1, lines 47-64).

Regarding claims 2 and 11, Caronni discloses that the gateway is located between a mobile computer and a computer in a wired network (see Fig. 2, where mobile unites 204 and 214 communicates with the computers in the network 107 through gateway 102).

Regarding claims 3 and 12, Caronni discloses the packet analysis device of the gateway extracts the keys (corresponding to the recited security association) from a field in the packet header provided by the sending computer (see col. 2, lines 40-50; col. 9, lines 19-49).

Regarding claims 4-6 and 13-15, Caronni discloses that the gateway may obtain the key information (corresponding to the recited security association) for cryptography operation on the transmitting packets from a database, which may be located on a server (see col. 9, lines 19-49; Fig. 3, 307).

Regarding claims 7, 8, 16 and 17, Caronni does not expressly disclose a mechanism for transferring information regarding the security association to a gateway belong to a network when a mobile terminals moves to an area covered by the network (i.e., visited network).

Inoue discloses that when a mobile computer moves from one network such as the home network to another network the gateway of the first network controls the security information regarding to the encryption process of the packets and transfers the

security information to the gateway of the visited network (see Figs. 2 and 6; col. 2, line 63-col. 3, line 23; col. 8, lines 33-67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include a mechanism (i.e., a handoff unit) in the gateway of the home network for handing over necessary security information to a next gateway as taught in Inoue in the system of Caronni when a mobile terminal moves to a visited network because it would improve the efficiency of encryption/decryption process of the transmitting packets (Inoue, col. 3, lines 23-49).

Regarding claims 9 and 18, Inoue discloses that the gateway in the home network of the mobile computer encapsulates the received IP packet and transmits to the gateway in the visited network (col. 6, lines 43-52). Inoue further discloses a mechanism to determine (corresponding to the recited judge) whether the security policy of the visited network is the same as the home network (see col. 2, line 63-col. 3, line 22). If the security policies are different the encryption process of the packets are performed at the mobile computer not by the gateway of the visited network. This means that packet relaying is occurred at the gateway of the visited network.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

February 8, 2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100